A2

1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI
(c) 2001 Derwent Info Ltd. All rts. reserv.

012182604 **Image available**
WPI Acc No: 1998-599517/**199851**
XRPX Acc No: N98-466907
Software security system in network - is incorporated into intelligent software module either as encryption, secret key or electronic signature
Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10269186	A	19981009	JP 9771311	A	19970325	199851	B

Priority Applications (No Type Date): JP 9771311 A 19970325
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10269186	A		6	G06F-015/16	

Abstract (Basic): JP 10269186 A
The security system is incorporated into an intelligent agent which is the software module itself, either by encryption, secret key or electronic signature.
ADVANTAGE - Prevents access to software key unauthorised users of software in network.
Dwg.1/6
Title Terms: SOFTWARE; SECURE; SYSTEM; NETWORK; INCORPORATE; INTELLIGENCE; SOFTWARE; MODULE; ENCRYPTION; SECRET; KEY; ELECTRONIC; SIGNATURE
Derwent Class: T01
International Patent Class (Main): G06F-015/16
International Patent Class (Additional): G06F-009/06; G06F-013/00
File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2000 JPO & JAPIO. All rts. reserv.

05986086 **Image available**
SECURITY PROTECTION SYSTEM FOR AGENT

PUB. NO.: 10-269186 A]
PUBLISHED: October 09, 1998 (19981009)
INVENTOR(s): IMAI KOUSUKE
APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-071311 [JP 9771311]
FILED: March 25, 1997 (19970325)
INTL CLASS: [6] G06F-015/16; G06F-009/06; G06F-013/00; G06F-013/00
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 45.1 (INFORMATION PROCESSING -- Arithmetic Sequence Units); 45.2 (INFORMATION PROCESSING -- Memory Units)

ABSTRACT

PROBLEM TO BE SOLVED: To prevent a third party from leaking secrecy or illegally using an intelligent agent by allowing the intelligent agent itself to have a security module and protect itself.

SOLUTION: A client machine selects and adds a necessary security mechanism 2 for the agent 1. The selected security mechanism 2 performs a necessary security process to obtain security information 3. The agent 1 moves to a server machine together with the data 4, a security mechanism 2, and security information that it has. The agent 1 after moving onto the server machine performs a security process with a service providing program 10, which provides service on the server machine. Consequently, both the client and server can protect the security without being aware of the security mechanisms that support the opposite sides.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－269186

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/16	３７０	Ｇ０６Ｆ	15/16	３７０Ｚ
	9/06	５５０		9/06	５５０Ｚ
	13/00	３５１		13/00	３５１Ｚ
		３５７			３５７Ｚ

審査請求　未請求　請求項の数１　ＯＬ　（全 ６ 頁）

(21)出願番号　特願平9－71311

(22)出願日　平成９年(1997)３月25日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　今井　厚祐
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　エージェントのセキュリティ保護方式

(57)【要約】
【課題】ネットワーク上のインテリジェントエージェントにおいて、エージェント自身のセキュリティを保護する必要がある。
【解決手段】エージェント自身にセキュリティモジュールとセキュリティ情報を持たせ、自分自身を保護する能力を持たせる。エージェントのセキュリティ保護を向上させ、またサーバでの不正なエージェントの実行防止などの効果を持つ。

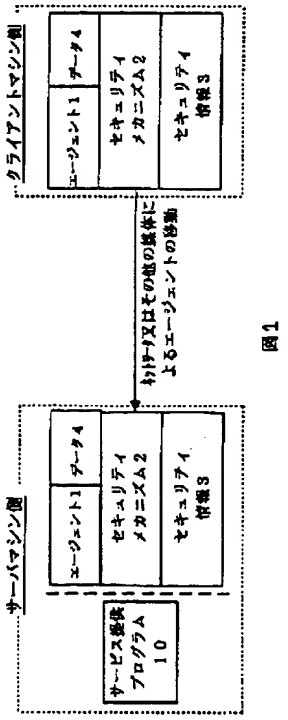

図1

1

【特許請求の範囲】

【請求項１】ネットワークを介して自己の判断で移動・実行するインテリジェントエージェントにおいて、エージェント自身がセキュリティモジュールを持ち、自分自身を保護することを特徴とするエージェントのセキュリティ管理方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】エージェントのセキュリティ保護方式に関する。

【０００２】

【従来の技術】エージェントは、自律性、移動性、知性を持つソフトウェアモジュールで、ユーザの依頼を受けると自分自身の判断でネットワーク上を移動し、アプリケーションを自動的に起動し、処理していく。現在、広く研究開発されているエージェント技術ではセキュリティ保護方式について考慮されていなかった。

【０００３】なお、本発明の出願前に知られている最も近い例としては、特公平８－２７７２６公報に記載されているエージェント・コンピュータ管理システムや特開平７－８７１１６公報に記載されているネットワークを管理する方法及び装置が提案されている。しかし、エージェント自身がセキュリティ機能を持つことについてはカバーされていない。

【０００４】

【発明が解決しようとする課題】従来のエージェント技術では、エージェント自身の持つデータの機密性保護、データへのアクセス制御、エージェントとデータの完全性保護、第三者によるエージェントモジュールの不正使用、エージェント起動者の識別、悪意を持つエージェントの実行の強制終了、複数セキュリティメカニズム・アルゴリズムサポートなどについて考慮されていなかったため、不特定多数と接続されている公衆回線などを介して移動、実行するエージェントのセキュリティ保護の問題があった。

【０００５】そこで本発明では、エージェント自身にセキュリティ機能を持たせることにより、エージェントのセキュリティ保護を高めることを考えた。

【０００６】本発明の目的は、エージェントの持つデータの機密生保護を提供することにある。

【０００７】本発明の他の目的は、エージェントの持つデータやエージェント自身へのアクセス制御機能を提供することにある。

【０００８】本発明の他の目的は、エージェントとデータの完全性保護を提供することにある。

【０００９】本発明の他の目的は、第三者によるエージェントモジュールの不正使用の防止機能を提供することにある。

【００１０】本発明の他の目的は、エージェント起動者を識別する機能を提供することにある。

2

【００１１】本発明の他の目的は、悪意を持つエージェントの実行を強制終了させる機能を提供することにある。

【００１２】本発明の他の目的は、複数セキュリティメカニズム・アルゴリズムをサポートする機能を提供することにある。

【００１３】

【課題を解決するための手段】本発明は、インテリジェントエージェント自身がセキュリティモジュールを持ち、自分自身を保護する手段が提供される。

【００１４】

【発明の実施の形態】図１は本発明の一実施例に基づくエージェントセキュリティを示す図である。本システムは、エージェント１、セキュリティメカニズム２、セキュリティ情報３、サービス提供プログラム１０からなる。

【００１５】クライアントマシンでは、エージェント１に対して必要なセキュリティメカニズム２を選択しエージェント１に追加する。セキュリティメカニズム２の選択方法として、　サービス提供者に関係なくエージェント起動側のディフォルトのメカニズムを選択する、　エージェント起動側に事前に登録されている、サービス提供者がサポートするメカニズムを選択する、　エージェント１を起動する前に、サーバマシン側、クライアントマシン側の間でサポートしているセキュリティメカニズムに関して折衝し、選択する、　各マシン又はプログラムは、ディレクトリサーバなどの第三者サーバに対してサポートしているセキュリティメカニズムを事前に登録し、クランアントマシン側はその第三者サーバに必要なセキュリティメカニズムを問い合わせることによって選択する。選択されたセキュリティメカニズム２は、必要なセキュリティ処理を行い、セキュリティ情報３を得る。エージェント１は、エージェント１が持つデータ４、セキュリティメカニズム２、セキュリティ情報３と共にサーバマシンへ移動する。エージェント１は、サーバマシン上に移動した後、サーバマシン上でサービスを提供するサービス提供プログラム１０との間でセキュリティ処理を行う。

【００１６】図１では、実施例としてクライアントマシン上でセキュリティメカニズム２を追加しているが、エージェント１にセキュリティメカニズム２を追加するためのサーバを使用することも可能である。

【００１７】セキュリティ処理が正常に終了した場合、エージェント１はサービス提供プログラム１０からサービスを受ける。

【００１８】次に図２を用いて本発明のセキュリティメカニズム２、セキュリティ情報３の具体的な構成とクライアントマシンでのセキュリティ処理方式を説明する。図２に示すように、図１のセキュリティメカニズム２は、ハッシュメカニズム２１、暗号・復号メカニズム２

２、鍵管理メカニズム２３、アクセス制御メカニズム２４から構成され、図１のセキュリティ情報３は、ハッシュ値３１、エージェント起動者の電子署名３２、電子鍵３３、アクセス制御情報３４から構成される。また、クライアントでは、事前に暗号・復号メカニズム２２の処理に必要な、起動者の秘密鍵３３３、サービス提供者の公開鍵３３２を保持しておく必要がある。

【００１９】ハッシュメカニズム２１は任意のデータに対してハッシュ計算を行い。ハッシュ値３１を算出する機能を持つモジュールである。

【００２０】暗号・復号メカニズム２２は任意のデータに対して暗号処理や電子署名３２の生成処理、または既に暗号処理されているデータに対して復号処理を行う機能を持つモジュールである。

【００２１】鍵管理メカニズム２３は暗号・復号・電子署名３２の生成処理に必要な電子鍵３３の生成、管理機能を持つモジュールである。

【００２２】アクセス制御メカニズム２４は、エージェント１自身やエージェント１が持つデータ４に対するアクセスを制御するために、アクセスを要求してくる要求者の身元とその要求者の持つアクセス制御情報３４から、アクセスを制御する機能を持つモジュールである。アクセス制御情報３４は、エージェント生成者又はエージェント起動者によってアクセス制御メカニズム２４に提供される。

【００２３】クライアントマシンでのセキュリティ処理方式について説明する。クライアントマシンのエージェント起動者は、先に記したセキュリティメカニズムや暗号アルゴリズムから必要なものを選択する。例として、図３を用いて全てのセキュリティメカニズムを選択した場合について説明する。

【００２４】まず初めに、ハッシュメカニズム２１は保護の対象となるデータのハッシュ値３１を算出する。この時に保護の対象となるデータは、エージェント１とデータ４であるが、必要に応じてハッシュメカニズム２１、暗号・復号メカニズム２２、鍵管理メカニズム２３、アクセス制御メカニズム２４、エージェント起動者の電子署名３２、電子鍵３３、アクセス制御情報３４もその対象となる。

【００２５】次に、クライアントのエージェント起動者またはエージェント生成者は、エージェント１の持つデータ４またはエージェント１、セキュリティメカニズム２、セキュリティ情報３に対するアクセス制御情報３４を生成する。

【００２６】次に鍵管理メカニズム２３は、データの暗号化に必要な電子鍵である共通鍵３３１を生成する。暗号・復号メカニズム２２は、この共通鍵３３１を使ってデータに暗号化処理を施す。この時に暗号化処理の対象となるデータは、エージェント１とエージェント１の持つデータ４であるが、必要に応じてハッシュ値３１、アクセス制御情報３４もその対象となる。共通鍵３３１によって暗号処理が終わった後、暗号・復号メカニズム２２は、その共通鍵３３１をサービス提供者の公開鍵３３２で暗号化処理したものが電子鍵３３となる。

【００２７】次に暗号・復号メカニズム２２はエージェント起動者の秘密鍵３３３を使って、データに対してエージェント起動者の電子署名３２を生成する。この時に対象となるデータは、エージェント１とエージェント１が持つデータ４であるが、必要に応じてハッシュメカニズム２１、暗号・復号メカニズム２２、鍵管理メカニズム２３、アクセス制御メカニズム２４、ハッシュ値３１、電子鍵３３、アクセス制御情報３４もその対象となる。

【００２８】全ての処理が終わった後、エージェント１はセキュリティメカニズム２とセキュリティ情報３と共にサーバマシンへ移動する。

【００２９】次に図４、図５、図６を用いて本発明のサーバマシンでのセキュリティ処理方式を説明する。図４に示すように、サーバマシン側では、先に説明したハッシュメカニズム２１、暗号・復号メカニズム２２、鍵管理メカニズム２３、アクセス制御メカニズム２４、ハッシュ値３１、エージェント起動者の電子署名３２、電子鍵３３、アクセス制御情報３４とサービス提供プログラム１０から構成される。また、サーバでは、事前に暗号・復号メカニズム２２やサービス提供プログラム１０の復号・電子署名識別処理に必要な、起動者の公開鍵３３５、サービス提供者の秘密鍵３３４を保持しておく必要がある。

【００３０】サービス提供プログラム１０は　エージェント１から要求のあるサービスを提供する機能、　エージェント起動者の電子署名の識別機能、　暗号化されたデータの復号処理機能、　エージェントを強制終了させる機能を持つモジュールである。

【００３１】図５、図６を使ってエージェントでのセキュリティ処理例を説明する。

【００３２】初めに、サービス提供プログラム１０はエージェント起動者の電子署名３２を起動者の公開鍵３３５を使って識別する。サービス提供プログラム１０は、この識別処理から誰が署名したかを確認し、その署名者からのエージェントを実行させて良いかどうかを判断する。必要ならエージェントを強制終了させる。

【００３３】次に、鍵管理メカニズム２３は電子鍵３３をサービス提供プログラム１０に渡す。サービス提供プログラム１０は受け取った電子鍵３３をサービス提供者の秘密鍵３３４で復号処理を行い、共通鍵３３１を入手し、鍵管理メカニズム２３に渡す。鍵管理メカニズム２３は、共通鍵３３１を暗号・復号メカニズム２２に渡す。暗号・復号メカニズム２２は、共通鍵３３１を使って暗号処理されているデータの復号を行う。データは、クライアントで暗号処理されたデータである。

【００３４】ハッシュメカニズム２１はデータに対するハッシュ値を計算し、転送されてきたハッシュ値３１と比較する。データは、クライアントでハッシュ処理されたデータである。

【００３５】サービス提供プログラム１０が、エージェント１、データ４、ハッシュメカニズム２１、暗号・復号メカニズム２２、鍵管理メカニズム２３、アクセス制御メカニズム２４、ハッシュ値３１、エージェント起動者の電子署名３２、電子鍵３３、アクセス制御情報３４に対してアクセス要求してきた場合、アクセス制御メカニズム２４はアクセス制御情報３４を基にアクセスを制御する。

【００３６】サーバマシン上にセキュリティメカニズム２でセキュリティ処理エラーが発生した場合、エージェント１は全ての処理を中断し、クライアントへ移動する。

【００３７】

【発明の効果】以上説明したように、本発明によれば、エージェント自身に暗号処理を施すことができるので、第三者による機密の漏洩やエージェントの不正使用を防ぐという効果がある。また、セキュリティメカニズムやアルゴリズムはエージェント自身が持ち、一緒に移動することができるので、クライアント、サーバとも相手がサポートしているセキュリティメカニズム、アルゴリズムを気にしないで、セキュリティを保護することができるという効果もある。また、アクセス制御メカニズムを持つことができるので、エージェントやそれが持つセキュリティメカニズム、セキュリティ情報へのアクセスを制御することができるという効果もある。また、エージェントと共に電子署名を送付できるので、サーバマシン側で不必要なエージェントの実行を制御できるという効果もある。また、本発明ではサービス提供プログラムは自分の秘密鍵をエージェント又はセキュリティメカニズムに渡さないシステムなので、秘密鍵の不正な複製、利用を防止できるという効果もある。さらに、本発明ではエージェントに対する電子署名はエージェント起動者のみとしているので、エージェントの起動者を識別することができるという効果もある。

【図面の簡単な説明】

【図１】本発明の一実施例に基づくエージェントセキュリティを示す図である。

【図２】クライアントマシンでのセキュリティ処理方式の一例を示す図である。

【図３】クライアントマシンでのセキュリティ処理の流れの一例を示す図である。

【図４】サーバマシンでのセキュリティ処理方式の一例を示す図である。

【図５】エージェントでのセキュリティ処理の流れの一例を示す図である。

【図６】サービス提供プログラムでのセキュリティ処理の流れの一例を示す図である。

【符号の説明】

１０…サービス提供プログラム、
２１…ハッシュメカニズム、
２２…暗号・復号メカニズム、
２３…鍵管理メカニズム、
２４…アクセス制御メカニズム、
３１…ハッシュ値、
３２…エージェント起動者の電子署名、
３３…電子鍵、
３４…アクセス制御情報、
３３１…共通鍵、
３３２…サービス提供者の公開鍵、
３３３…起動者の秘密鍵、
３３４…サービス提供者の秘密鍵、
３３５…起動者の公開鍵。

【図１】

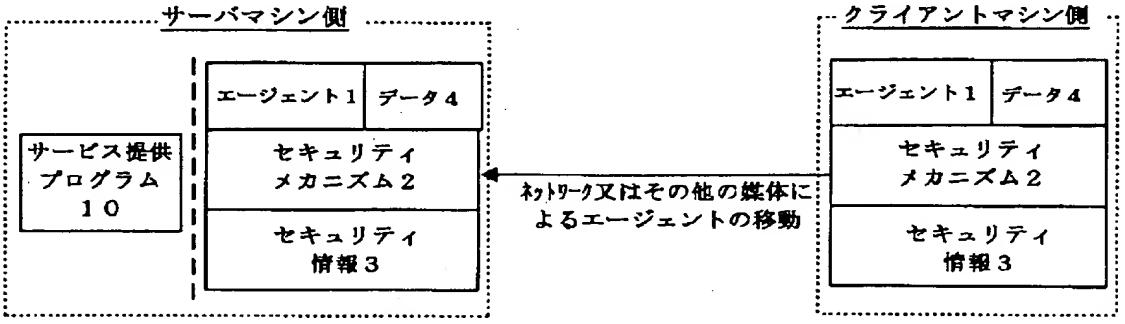

図１

【図２】

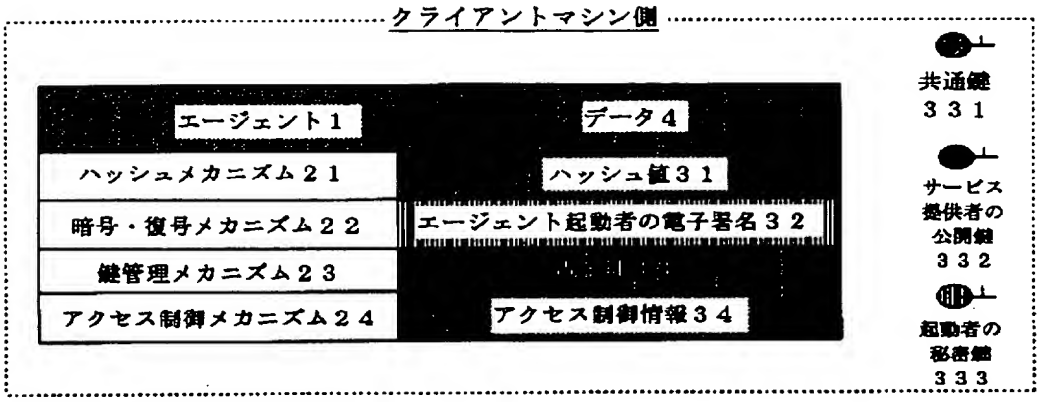

図２

【図３】

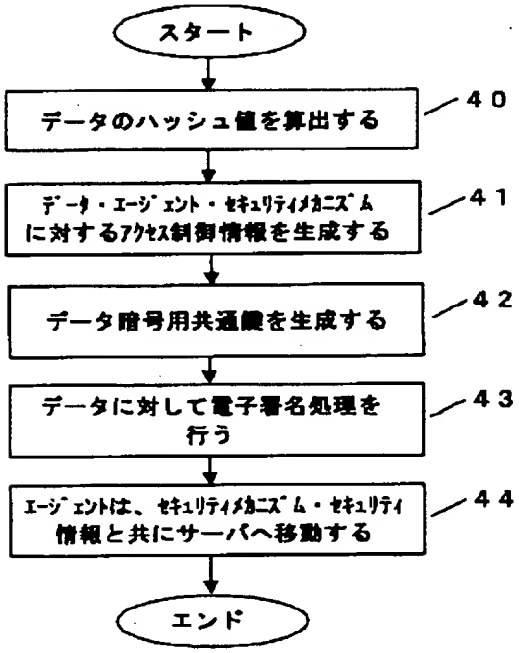

図３

【図５】

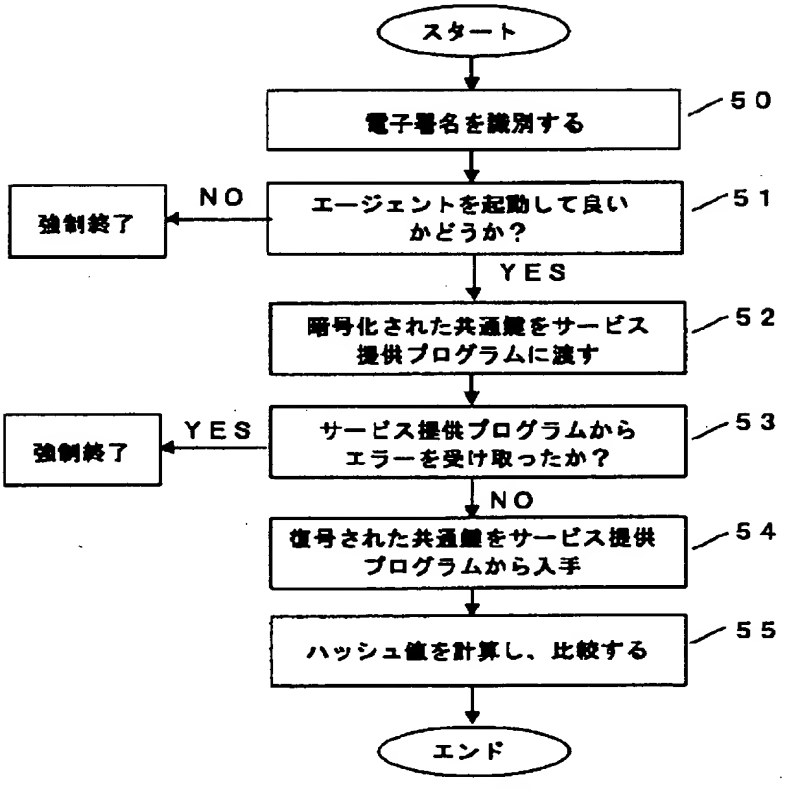

図５

【図４】

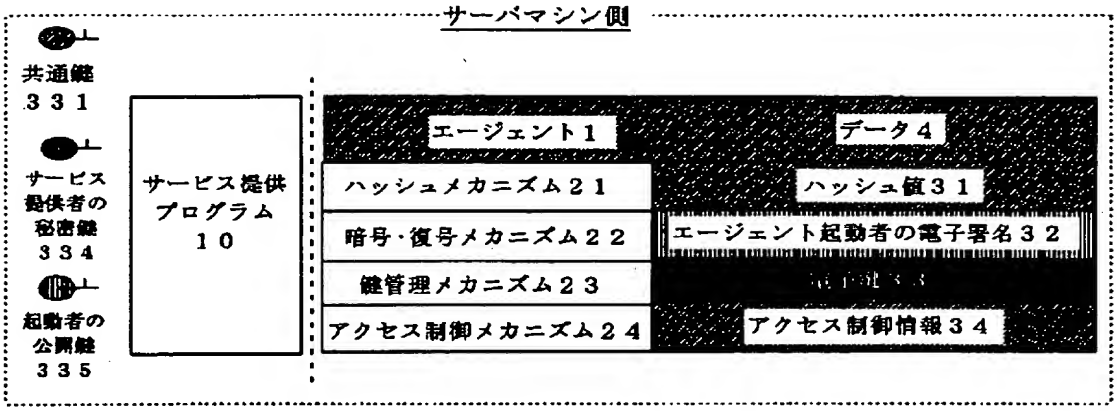
サーバマシン側
共通鍵
３３１
サービス
提供者の
秘密鍵
３３４
起動者の
公開鍵
３３５
サービス提供
プログラム
１０
エージェント１
ハッシュメカニズム２１
暗号・復号メカニズム２２
鍵管理メカニズム２３
アクセス制御メカニズム２４
データ４
ハッシュ値３１
エージェント起動者の電子署名３２
アクセス制御情報３４

図4

【図６】

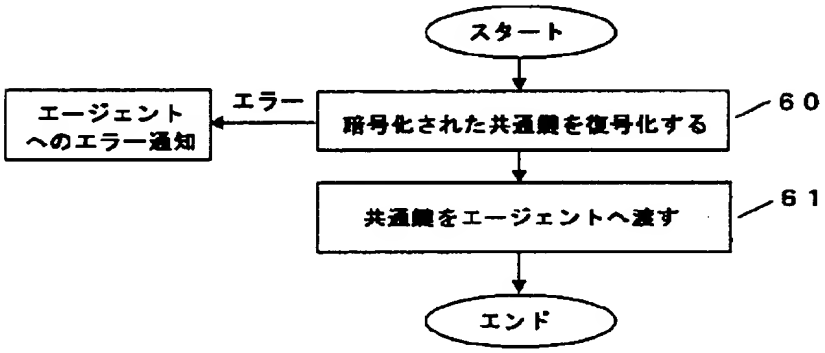
スタート
暗号化された共通鍵を復号化する
６０
エラー
エージェント
へのエラー通知
共通鍵をエージェントへ渡す
６１
エンド

図6